Published before January 2001
Terms used **sealed enclosure key exchange**

Found **3** of **112,590**

Sort results by: relevance
Display results: expanded form

Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 3 of 3

Relevance scale

1 Technical reports
SIGACT News Staff
January 1980 **ACM SIGACT News**, Volume 12 Issue 1
Full text available: pdf(5.28 MB) Additional Information: full citation

2 Functional Specifications for Typewriter-Like Time-Sharing Terminals
T. A. Dolotta
January 1970 **ACM Computing Surveys (CSUR)**, Volume 2 Issue 1
Full text available: pdf(2.45 MB) Additional Information: full citation, references, citings, index terms

3 d1-optimal motion for a rod (extended abstract)
Tetsuo Asano, David Kirkpatrick, Chee K. Yap
May 1996 **Proceedings of the twelfth annual symposium on Computational geometry**
Full text available: pdf(1.14 MB) Additional Information: full citation, references, citings, index terms

Results 1 - 3 of 3

181 Mobile IP and the IETF
Charles E. Perkins
April 2000 **ACM SIGMOBILE Mobile Computing and Communications Review**, Volume 4 Issue 2
Full text available: pdf(631.96 KB) Additional Information: full citation, index terms

182 An overview of the University of Texas at Dallas' center for advanced telecommunications systems and services (CATSS)
Imrich Chlamtac, Stefano Basagni, Stephen Gibbs
April 2000 **ACM SIGMOBILE Mobile Computing and Communications Review**, Volume 4 Issue 2
Full text available: pdf(816.71 KB) Additional Information: full citation, abstract, index terms

The University of Texas at Dallas' Center for Advanced Telecommunications Systems and Services (CATSS) was founded in January 1998 to satisfy the acute needs of the growing Dallas/Richardson telecommunications industry. Its mission is to foster a strong Industry-University partnership to advance local telecommunications industries to the next generation of systems and products. Composed of UTD faculty and industry researchers and managers, the Center's focus is exclusively telecommunications-rel ...

183 A report on the IEEE 802 plenary meeting Kauai, HI, USA
Victor Bahl
January 2000 **ACM SIGMOBILE Mobile Computing and Communications Review**, Volume 4 Issue 1
Full text available: pdf(842.71 KB) Additional Information: full citation, index terms

184 Wireless personal area networks: an overview of the IEEE P802.15 working group
Richard C. Braley, Ian C. Gifford, Robert F. Heile
January 2000 **ACM SIGMOBILE Mobile Computing and Communications Review**, Volume 4 Issue 1
Full text available: pdf(1.04 MB) Additional Information: full citation, index terms

185 Efficient verifiable encryption (and fair exchange) of digital signatures
Giuseppe Ateniese
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**
Full text available: pdf(781.40 KB) Additional Information: full citation, abstract, references, citings, index terms

A fair exchange protocol allows two users to exchange items so that either each user gets the other's item or neither user does. In [2], verifiable encryption is introduced as a primitive that can be used to build extremely efficient fair exchange protocols where the items exchanged represent

digital signatures. Such protocols may be used to digitally sign contracts.This paper presents new simple schemes for verifiable encryption of digital signatures. We make us ...

Keywords: contract signing problem, digital signatures, fair exchange, proof of knowledge, public-key cryptography, verifiable encryption

186 Public-key cryptography and password protocols: the multi-user case 

Maurizio Kliban Boyarsky

November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**

Full text available: pdf(1.00 MB) Additional Information: full citation, abstract, references, citings, index terms

The problem of password authentication over an insecure network when the user holds only a human-memorizable password has received much attention in the literature. The first rigorous treatment was provided by Halevi and Krawczyk, who studied off-line password guessing attacks in the scenario in which the authentication server possesses a pair of private and public keys. In this work we: Show the inadequacy of both the HK formalization and protocol in the ...

187 A public-key based secure mobile IP 

John Zao, Joshua Gahm, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan, Isidro Castineyra, Stephen Kent

October 1999 **Wireless Networks**, Volume 5 Issue 5

Full text available: pdf(255.65 KB) Additional Information: full citation, references, citings, index terms

188 Public-key cryptography and password protocols 

Shai Halevi, Hugo Krawczyk

August 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 3

Full text available: pdf(275.84 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We study protocols for strong authentication and key exchange in asymmetric scenarios where the authentication server possesses ~a pair of private and public keys while the client has only a weak human-memorizable password as its authentication key. We present and analyze several simple password authentication protocols in this scenario, and show that the security of these protocols can be formally proven based on standard cryptographic assumptions. Remarkably, our analysis shows optimal re ...

Keywords: dictionary attacks, hand-held certificates, key exchange, passwords, public passwords, public-key protocols

189 Mobile IP and the IETF 

Charles E. Perkins

July 1999 **ACM SIGMOBILE Mobile Computing and Communications Review**, Volume 3 Issue 3

Full text available:

pdf(466.87 KB) Additional Information: full citation, index terms

190 Public-key cryptography and password protocols
Shai Halevi, Hugo Krawczyk
November 1998 **Proceedings of the 5th ACM conference on Computer and communications security**
Full text available: pdf(1.28 MB) Additional Information: full citation, references, citings, index terms

191 Communication complexity of group key distribution
Klaus Becker, Uta Wille
November 1998 **Proceedings of the 5th ACM conference on Computer and communications security**
Full text available: pdf(660.80 KB) Additional Information: full citation, references, citings, index terms

192 A modular approach to the design and analysis of authentication and key exchange protocols (extended abstract)
Mihir Bellare, Ran Canetti, Hugo Krawczyk
May 1998 **Proceedings of the thirtieth annual ACM symposium on Theory of computing**
Full text available: pdf(1.61 MB) Additional Information: full citation, references, citings, index terms

193 Strong password-only authenticated key exchange
David P. Jablon
October 1996 **ACM SIGCOMM Computer Communication Review**, Volume 26 Issue 5
Full text available: pdf(1.52 MB) Additional Information: full citation, abstract, citings, index terms

A new simple password exponential key exchange method (SPEKE) is described. It belongs to an exclusive class of methods which provide authentication and key establishment over an insecure channel using only a small password, without risk of offline dictionary attack. SPEKE and the closely-related Diffie-Hellman Encrypted Key Exchange (DH-EKE) are examined in light of both known and new attacks, along with sufficient preventive constraints. Although SPEKE and DH-EKE are similar, the constraints a ...

194 Refinement and extension of encrypted key exchange
Michael Steiner, Gene Tsudik, Michael Waidner
July 1995 **ACM SIGOPS Operating Systems Review**, Volume 29 Issue 3
Full text available: pdf(553.70 KB) Additional Information: full citation, abstract, citings, index terms

In their recent paper, "Encrypted Key Exchange: Password-based Protocols Secure Against Dictionary Attacks," Bellovin and Merritt propose a novel and elegant method for safeguarding weak passwords. This paper discusses

a possible weakness in the proposed protocol, develops some enhancements and simplifications, and provides a security analysis of the resultant *minimal* EKE protocol. In addition, the basic 2-party EKE model is extended to the 3-party setting; this yields a protocol with som ...

195 Towards acceptable key escrow systems

Thomas Beth, Hans-Joachim Knobloch, Marcus Otten, Gustavus J. Simmons, Peer Wichmann

November 1994 **Proceedings of the 2nd ACM Conference on Computer and communications security**

Full text available: pdf(833.24 KB) Additional Information: full citation, abstract, references, citings, index terms

Escrowed Key Cryptosystems hold the promise of faithfully realizing legal guarantees of privacy for users under normal circumstances while at the same time insuring that privacy can be breached by authorities in special circumstances under appropriate legal safeguards. The most attractive feature of these schemes is that it is possible to ensure that the interests of each of the parties—the users, the law enforcement or national security agencies, the court or other monitoring entitie ...

196 Extending cryptographic logics of belief to key agreement protocols

Paul van Oorschot

December 1993 **Proceedings of the 1st ACM conference on Computer and communications security**

Full text available: pdf(1.35 MB) Additional Information: full citation, abstract, references, citings, index terms

The authentication logic of Burrows, Abadi and Needham (BAN) provided an important step towards rigourous analysis of authentication protocols, and has motivated several subsequent refinements. We propose extensions to BAN-like logics which facilitate, for the first time, examination of public-key based authenticated key establishment protocols in which both parties contribute to the derived key (i.e. key agreement protocols). Attention is focussed on six distinct generic goals for authenti ...

197 Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password file compromise

Steven M. Bellovin, Michael Merritt

December 1993 **Proceedings of the 1st ACM conference on Computer and communications security**

Full text available: pdf(620.09 KB) Additional Information: full citation, abstract, references, citings, index terms

The encrypted key exchange (EKE) protocol is augmented so that hosts do not store cleartext passwords. Consequently, adversaries who obtain the one-way encrypted password file may (i) successfully mimic (spoof) the host to the user, and (ii) mount dictionary attacks against the encrypted passwords, but cannot mimic the user to the host. Moreover, the important security properties of EKE are preserved—an active network attacker obtains insufficient information to mount dictionary attac ...

198 On key distribution protocols for repeated authentication

Paul Syverson

October 1993 **ACM SIGOPS Operating Systems Review**, Volume 27 Issue 4

Full text available: pdf(698.23 Additional Information: full citation, abstract, citings, index

KB) terms

In [KSL92], Kehne et al. present a protocol (KSL) for key distribution. Their protocol allows for repeated authentication by means of a ticket. They also give a proof in BAN logic [BAN89] that the protocol provides the principals with a reasonable degree of trust in the authentication and key distribution. They present an optimality result that their protocol contains a minimal number of messages. Nonetheless, in [NS93] Neuman and Stubblebine present a protocol (NS) as an explicit alternative to ...

199 An efficient protocol for unconditionally secure secret key exchange 

Michael J. Fischer, Rebecca N. Wright

January 1993 **Proceedings of the fourth annual ACM-SIAM Symposium on Discrete algorithms**

Full text available: pdf(907.75 KB) Additional Information: full citation, references, citings, index terms

200 How to exchange (secret) keys 

Manuel Blum

May 1983 **ACM Transactions on Computer Systems (TOCS)**, Volume 1 Issue 2

Full text available: pdf(1.25 MB) Additional Information: full citation, references, citings, index terms

Keywords: cryptography, factorization, protocols, public key encryption, secrets, security, transaction protection protocols

Results 181 - 200 of 200 Result page: previous 1 2 3 4 5 6 7 8 9 **10**